Glossary

access control entry (ACE) — An entry within an Access Control List that grants or denies permissions to users or groups for a given resource.

Access Control List (ACL) — Contains a set of access control entries that define an object's permission settings. ACLs enable administrators to explicitly control access to resources.

Active Directory — The Windows 2000 directory service that replaces the antiquated Windows NT domain structure. Active Directory forms the basis for centralized network management on Windows 2000 networks, providing a hierarchical view of network resources.

Active Directory Service Interface (ADSI) — A directory service model implemented as a set of COM interfaces. ADSI allows Windows applications to access Active Directory, often through ActiveX interfaces such as VBScript.

Active Directory Users and Computers — The primary systems administrator utility for managing users, groups, and computers in a Windows 2000 domain, implemented as a MMC snap-in.

address (A) record — The most basic type of resource record on a DNS server. Every client that registers with DNS has an associated A record that maps its name to its IP address.

assigned applications — Applications that are always available to the user, even if the user attempts to uninstall them. Through the Software Installation utility in Group Policy, administrators can assign applications to users.

asynchronous processing — Occurs when one task waits until another is finished before beginning. It is typically associated with scripts—for example, a user logon script that does not run before the computer startup script has completed. This is the default behavior in Windows 2000.

attribute — The basic unit of an object. An attribute is a single property that, through its values, defines an object. For example, the account name is an attribute of a standard user account.

auditing — A security process that tracks the usage of selected network resources, typically storing the results in a log file.

authentication — The process by which a user's logon credentials are validated by a server so that access to a network resource can be granted or denied.

AXFR — A DNS term that refers to a request from a primary server to one or more secondary servers for a full zone transfer.

Backup Domain Controller (BDC) — A Windows NT 3.*x* and 4 server that contains a backup copy of the domain security accounts manager (user account and security information). BDCs take load from the Primary Domain Controller by servicing logon requests. Periodic synchronizing ensures that data between the PDC and BDCs remains consistent.

baseline — A term associated with performance monitoring. A baseline is the initial result of monitoring by which all future results are measured.

bridgehead server — The contact point for the exchange of directory information between Active Directory sites.

caching — The process by which name resolution query results are stored in order to speed up future name resolution for the same destinations.

checkpoint file — Indicates the location of the last information successfully written from the transaction logs to the database. In a data recovery scenario, the checkpoint file indicates where the recovery or replaying of data should begin.

circular logging — The process by which a full log file is overwritten with new data, rather than a new log file being created. Circular logging conserves disk space but can result in data loss in a disaster-recovery scenario.

computer configuration — The portion of a Group Policy Object that allows for computer policies to be configured and applied.

container — An object in Active Directory that is capable of holding other objects. An example of a container would be the Users folder in Active Directory Users and Computers.

convergence — The process of stabilization after network changes occur. Often associated with routing or replication, convergence ensures that each router or server contains consistent information.

counters — The metrics that are used in performance monitoring. Counters are what you are actually monitoring. An example of a counter for a CPU object would be %Processing Time.

CScript — The command-line executable for Windows Scripting Host.

dcpromo — The command-line utility that is used to promote a Windows 2000 server to a domain controller.

delegation — The process of offloading the responsibility for a given task or set of tasks to another user or group. Delegation in Windows 2000 usually involves granting permission to someone else to perform a specific administrative task, such as creating computer accounts.

directory — A database that contains any number of different types of data. In Windows 2000, the Active Directory contains information about objects in the domain such as computers, users, groups, and printers.

directory service — Provides the methods of storing directory data and making that data available to other directory objects.

Directory System Agent (DSA) — Makes data within Active Directory accessible to applications that want it, acting as a liaison between the directory database and the applications.

disk quota — An administrative limit set on the server storage space that can be used by any particular user.

distinguished name — The name that uniquely identifies an object, using the relative distinguished name, domain name, and the container holding the object. For example, the distinguished name CN=WWillis, CN=Inside-Corner, CN=COM refers to the WWillis user account in the inside-corner.com domain.

Distributed File System (Dfs) — A Windows 2000 service that allows resources from multiple server locations to be presented through Active Directory as a contiguous set of files and folders, resulting in greater ease of use for users of network resources.

distribution point — The network shared location for software to be stored for the purpose of making it available for installation to users.

domain — A collection of Windows 2000 computers, users, and groups that share a common directory database. Domains are defined by an administrator.

domain controller (DC) — A server that is capable of performing authentication. In Windows 2000, a DC holds a copy of the Active Directory database.

domain local group — Can contain other domain local groups from its own domain, as well as global groups from any domain in the forest. Domain local groups can be used to assign permissions for resources located in the same domain as the group.

Domain Name System (DNS) — A hierarchical name resolution system that resolves host names into IP addresses and vice versa.

Dynamic Domain Name System (DDNS) — An extension of DNS that allows Windows 2000 Professional systems to automatically register their A records with DNS at the time they obtain an IP address from a DHCP server.

Dynamic Host Configuration Protocol (DHCP) — A service that allows an administrator to specify a range of valid IP addresses to be used on a network, as well as exceptions. These addresses are automatically given out to computers configured to use DHCP as they boot up on the network, saving the administrator from having to configure static IP addresses on each individual network device.

Encrypted File System (EFS) — A Windows 2000 feature that allows files and folders to be encrypted on NTFS partitions, protecting them from being read by other people.

Extensible Storage Engine (ESE) — The Active Directory database engine. ESE is an improved version of the older Jet database technology.

File Replication Service (FRS) — A service that provides multi-master replication between specified domain controllers within an Active Directory tree.

File Transfer Protocol (FTP) — A standard TCP/IP utility that allows for the transfer of files from an FTP server to a machine running the FTP client.

firewall — A hardware and software security system that functions to limit access to network resources across subnets. Typically, a firewall is used between a private network and the Internet to prevent outsiders from accessing the private network and to limit the Internet services that users of the private network can access.

flat namespace — A namespace that cannot be partitioned to produce additional domains. Windows NT 4 and earlier domains were examples of flat namespaces, as opposed to the Windows 2000 hierarchical namespaces.

folder redirection — A Windows 2000 feature that allows special folders such as My Documents on local Windows 2000 Professional system hard drives to be redirected to a shared network location.

forest — A grouping of Active Directory trees that have a trust relationship between them. Forests can consist of noncontiguous name-spaces; and unlike domains and trees, forests do not have to be given a specific name.

forward lookup query — A DNS name resolution process by which a host name is resolved to an IP address.

fully qualified domain name (FQDN) — A DNS domain name that unambiguously describes the location of the host within a domain tree. An example of an FQDN would be the computer www.inside-corner.com.

Global Catalog (GC) — Contains a partial replica of every Windows 2000 domain within the Active Directory, enabling users to find any object in the directory. The partial replica contains the most commonly used attributes of an object, as well as information on how to locate a complete replica elsewhere in the directory, if needed.

Global Catalog Server — The Windows 2000 server that holds the Global Catalog for the forest.

global group — Can contain users from the same domain as the group. Global groups can be added to domain local groups in order to control access to network resources.

Globally Unique Identifier (GUID) — A hexadecimal number supplied by the manufacturer of a product, which uniquely identifies the hardware or software. A GUID is in the form of 8 characters followed by 4, by 4, by 4, by 12. For example, {15DEF489-AE24-10BF-C11A-00BB844CE637} is a valid format for a GUID (braces included).

Group Policy — The Windows 2000 feature that allows for policy creation that affects domain users and computers. Policies can be anything from desktop settings to application assignment to security settings and more.

Group Policy Editor — The MMC snap-in that is used to modify the settings of a Group Policy Object.

Group Policy Object (GPO) — A collection of policies that apply to a specific target, such as the domain itself (default domain policy) or an OU. GPOs are modified through the Group Policy Editor to define policy settings.

hierarchical namespace — A namespace, such as that used with DNS, that can be partitioned in the form of a tree. This feature allows great flexibility in using a domain name, because any number of subdomains can be created under a parent domain.

host ID — The portion of an IP address that defines the host, as determined by the subnet mask. For example, if a host has an IP address of 192.168.1.20 and a subnet mask of 255.255.255.0, the host ID would be 20.

HOSTS — A static file that was the primary means for TCP/IP name resolution prior to DNS. The HOSTS file contains a list of host-to-IP-address mappings; it had to exist on every host computer that participates on a network. It has been replaced by the more manageable DNS service on all but the smallest of networks.

image — The installation source for Windows 2000 Professional and any optional applications created through the RIS RIPrep utility.

inheritance — The process by which an object obtains settings information from a parent object.

IntelliMirror — A collection of Windows 2000 technologies that provide for a comprehensive change and control management system.

IXFR — A DNS process by which a primary DNS server requests an incremental zone transfer from one or more secondary servers.

JavaScript (JScript) — An active scripting language that can be used in Windows 2000 with the Windows Scripting Host to run more complicated scripts than were available in the past through batch files.

just-in-time (JIT) — Technology that allows software features to be updated at the time they are accessed. Whereas in the past missing application features had to be installed manually, JIT technology allows the features to be installed on the fly as they are accessed, with no other intervention required.

Kerberos — An Internet standard security protocol that has largely replaced the older LAN Manager user authentication mechanism from earlier Windows NT versions.

Knowledge Consistency Checker (KCC) — A Windows 2000 service that functions to ensure that consistent database information is kept across all domain controllers. It attempts to ensure that replication can always take place.

latency — The delay that occurs in replication from the time a change is made to one replica until that change is applied to all other replicas in the directory.

Lightweight Directory Access Protocol (LDAP) — The Windows 2000 protocol that allows access to Active Directory. LDAP is an Internet standard for accessing directory services.

LMHOSTS — A static file used for NetBIOS name resolution. Similar to a HOSTS file, LMHOSTS had to exist on every individual computer on a network, making it increasingly difficult to keep up to date as the size of networks grew. LMHOSTS was essentially replaced by WINS on Windows networks prior to Windows 2000.

local-area network (LAN) — A network in which all hosts are connected over fast connections (4Mbps or greater for Token Ring, 10Mbps or better for Ethernet).

local group policy objects — Objects that exist on the local Windows 2000 system and take precedence over site-, domain-, and OU-applied GPOs.

Mail Exchanger (MX) record — A DNS record that defines an e-mail server.

Microsoft Management Console (MMC) — An extensible management framework that provides a common look and feel to all Windows 2000 utilities.

mixed mode — Allows Windows NT 4 domain controllers to exist and function within a Windows 2000 domain. This is the default setting when Active Directory is installed, although it can be changed to native mode.

multi-master replication — A replication model in which any domain controller will replicate data to any other domain controller. This is the default behavior in Windows 2000. It contrasts

with the single-master replication model of Windows NT 4, in which a PDC contained the master copy of everything and BDCs contained backup copies.

name resolution — The process of resolving a host name into a format that can be understood by computers. This format is typically an IP address, but it could also be a MAC address on non-TCP/IP networks.

namespace — A collection of resources that have been defined using some common name. The DNS namespace is hierarchical and can be partitioned, whereas Windows NT 4 and earlier used a flat namespace.

native mode — The mode in effect when all domain controllers in a domain have been upgraded to Windows 2000 and no more NT 4 domain controllers exist. An administrator explicitly puts Active Directory into native mode, at which time it cannot be returned to mixed mode without removing and reinstalling Active Directory.

NetBIOS — An application programming interface (API) used on Windows NT 4 and earlier networks by services requesting and providing name resolution and network data management.

network ID — The portion of an IP address that defines the network, as determined by the subnet mask. For example, if a host has an IP address of 192.168.1.20 and a subnet mask of 255.255.255.0, the network ID would be 192.168.1.

network operating system (NOS) — A generic term that applies to any operating system with built-in networking capabilities. All Windows operating systems beginning with Windows 95 have been true network operating systems.

non-local Group Policy Objects — GPOs that are stored in Active Directory rather than on the local machine. These can be site-, domain-, or OU-level GPOs.

nslookup — A TCP/IP utility used in troubleshooting DNS name resolution problems.

NTFS — The Windows NT/2000 file system that supports a much more robust feature set than FAT16 or FAT32 (used on Windows 9*x*). It is recommended that you use NTFS whenever possible on Windows 2000 systems.

object — A distinct entity represented by a series of attributes within Active Directory. An object can be a user, computer, folder, file, printer, and so forth.

object identifier — A number that uniquely identifies an object class or attribute. In the United States, the American National Standards Institute (ANSI) issues object identifiers, which take the form of a x.x.x.x dotted decimal format. Microsoft, for example, was issued the root object identifier of 1.2.840.113556, from which it can create further sub–object identifiers.

operations master — A Windows 2000 domain controller that has been assigned one or more of the special Active Directory domain roles, such as schema master, domain naming master, PDC emulator master, infrastructure master, and relative ID master.

Organizational Unit (OU) — An Active Directory container object that allows an administrator to logically group users, groups, computers, and other OUs into administrative units.

package — A collection of software compiled into a distributable form, such as a Windows Installer (.msi) package created with WinINSTALL.

parent-child trust relationship — The relationship in which a child object trusts its parent object, and a parent object is trusted by all child objects under it. Active Directory automatically creates two-way trust relationships between parent and child objects.

patching — The process of modifying or updating software packages.

ping — A TCP/IP utility that tests for basic connectivity between the client machine running ping and any other TCP/IP host.

policy — Settings and rules that are applied to users or computers—usually Group Policy in Windows 2000 and System Policy in Windows NT 4.

Pre-Boot Execution Environment (PXE) — A set of industry standards that allows for network commands to be run on a client computer before it has booted up in a traditional manner. PXE is used with RIS in Windows 2000 to install Windows 2000 Professional images on client computers.

Primary Domain Controller (PDC) — A Windows NT 4 and earlier server that contained the master copy of the domain database. PDCs authenticate user logon requests and track security-related changes within the domain.

Public Key Infrastructure (PKI) — Industry standard technology that allows for the establishment of secure communication between hosts based on a public key–private key or certificate-based system.

published applications — Applications that appear in Add/Remove Programs and that can be optionally installed by the user. Through the Software Installation utility in Group Policy, administrators can publish applications to users.

Registry — A data repository stored on each computer that contains information about that computer's configuration. The Registry is organized into a hierarchical tree and is made up of hives, keys, and values.

relative distinguished name (RDN) — The part of a DNS name that defines the host. For example, in the FQDN www.inside-corner.com, www is the relative distinguished name.

Remote Installation Services (RIS) — A Windows 2000 optional component that allows for the remote installation of Windows 2000 Professional onto compatible client computers.

replica — A copy of any given Active Directory object. Each copy of an object stored on multiple domain controllers is a replica.

replication — The process of copying data from one Windows 2000 domain controller to another. Replication is a process managed by an administrator, and it typically occurs automatically whenever changes are made to a replica of an object.

Request for Comments (RFC) — Official documents that specify Internet standards for the TCP/IP protocol.

resource records (RR) — Standard database record types used in DNS zone database files. Common types of resource records include Address (A), Mail Exchanger (MX), Start of Authority (SOA), and Name Server (NS), among others.

return on investment (ROI) — A business term that seeks to determine the amount of financial gain that occurs as a result of a certain expenditure. Many IT personnel today are faced with the prospect of justifying IT expenses in terms of ROI.

reverse lookup query — A DNS name resolution process by which an IP address is resolved to a host name.

root server — A DNS server that is authoritative for the root zone of a namespace.

router — A dedicated network hardware appliance or server running routing software and multiple network cards. Routers join dissimilar network topologies (such as Ethernet to Frame Relay) or simply segment networks into multiple subnets.

scalability — A measurement (often subjective) of how well a resource (such as a server) can expand to accommodate growing needs.

schema — In Active Directory, a description of object classes and attributes that the object class must possess and can possess.

schema master — The Windows 2000 domain controller that has been assigned the operations master role to control all schema updates within a forest.

security identifier (SID) — A number that uniquely identifies a user, group, or computer account. Every account is issued an SID when created, and if the account is later deleted and re-created with the same name, it will have a different SID. Once a SID is used in a domain, it can never be used again.

security templates — Collections of standard settings that can be applied administratively to give a consistent level of security to a system.

Single Instance Store (SIS) — An RIS component that combines duplicate files to reduce storage requirements on the RIS server.

single-master operations — Certain Active Directory operations that are allowed to occur in only one place at any given time (as opposed to being allowed to occur in multiple locations simultaneously). Examples of single-master operations include schema modification, PDC elections, and infrastructure changes.

site — A well-connected TCP/IP subnet.

site link — A connection between sites. Site links are used to join multiple locations.

slow link — A connection between sites that is not fast enough to provide full functionality in an acceptable timeframe. Site connections below 512Kbps are defined as slow links in Windows 2000.

snap-in — A component that can be added or removed from an MMC console to provide specific functionality. The Windows 2000 administrative tools are implemented as snap-ins.

Software Installation — A Group Policy component that allows administrators to optionally assign or publish applications to be available to users and computers.

Start of Authority (SOA) record — The first record created on a DNS server. The SOA record defines the starting point for a zone's authority.

static IP address — Also called a static address. A network device (such as a server) is manually configured with an IP address that doesn't change, rather than obtaining an address automatically from a DHCP server.

store — The physical storage of each Active Directory replica. A store is implemented using the Extensible Storage Engine.

subnet — A collection of hosts on a TCP/IP network that are not separated by any routers. A basic corporate LAN with one location would be referred to as a subnet when it is connected by a router to another network, such as that of an Internet service provider.

subnet mask — Defines where the network ID ends and the host ID begins in an IP address. Subnet masks can result in very basic to very complex network configurations, depending on their value.

synchronous processing — Occurs when one task does not wait for another to complete before it begins, but rather runs concurrently. Synchronous processing is typically associated with scripts in Windows 2000, such as when a user logon script runs without waiting for the computer startup script to finish.

system policies — Windows NT 4 Registry-based policy settings, which have largely been replaced in Windows 2000 by Group Policy. System policies can still be created using poledit.exe, however, for backward compatibility with non–Windows 2000 clients.

Systems Management Server (SMS) — A product in Microsoft's BackOffice server line that provides more extensive software distribution, metering, inventorying, and auditing than is possible strictly through Intellimirror.

TCP/IP — Transmission Control Protocol/Internet Protocol. TCP/IP is the standard protocol for communicating on the Internet and is the default protocol in Windows 2000.

Time To Live (TTL) — The amount of time a packet destined for a host will exist before it is deleted from the network. TTLs are used to prevent networks from becoming congested with packages that cannot reach their destinations.

total cost of ownership (TCO) — A change and control management concept that many IT professionals are being forced to become more aware of. TCO refers to the combined hard and soft costs (initial price and support costs) of owning a given resource.

transitive trust — An automatically created trust in Windows 2000 that exists between domain trees within a forest and between domains within a tree. Transitive trusts are two-way trust relationships.

tree — A collection of Windows 2000 domains that are connected through transitive trusts and that share a common Global Catalog and schema. Domains within a tree must form a contiguous namespace.

Universal group — A new Windows 2000 security group that can be used anywhere within a domain tree or forest. The only caveat is that Universal groups can be used only when Windows 2000 has been converted to native mode.

Update Sequence Number (USN) — A 64-bit number that keeps track of changes as they are written to copies of the Active Directory. As changes are made, this number increments by one.

user configuration — The portion of a Group Policy Object that allows for user policy settings to be configured and applied.

user profile — Contains settings that define the user environment, typically applied when the user logs on to the system.

Visual Basic Script (VBScript) — An active scripting language that can be used in Windows 2000 with the Windows Scripting Host to run more complicated scripts than have been available in the past through batch files. VBScript has been in the news frequently lately due to its use in creating e-mail viruses.

well-connected — A network that contains only fast connections between domains and hosts. The definition of *fast* is somewhat subjective and may vary from organization to organization.

wide-area network (WAN) — Multiple networks connected by slow connections between routers. WAN connections are typically 1.5Mbps or less.

Windows Internet Naming Service (WINS) — A dynamic name resolution system that resolves NetBIOS names to IP addresses on Windows TCP/IP networks. With Windows 2000, WINS is being phased out in favor of DNS.

Windows Management Instrumentation (WMI) — A Windows 2000 management infrastructure for monitoring and controlling system resources.

Windows Scripting Host (WSH) — Enables the running of VBScript or JavaScript scripts natively on a Windows system, offering increased power and flexibility over traditional batch files.

WinINSTALL — An optional utility that ships with Windows 2000 server and that can be used to create Windows Installer packages.

WScript — The Windows interface to the Windows Scripting Host.

X.500 — A set of standards developed by the International Standards Organization (ISO) that define distributed directory services.

zone — A subtree of the DNS database that can be managed as a single, separate entity from the rest of the DNS namespace.

zone file — The DNS database, traditionally stored as a text file on the primary server and replicated to secondary servers. With Windows 2000, the zone file can be optionally integrated into Active Directory.

zone transfer — The DNS process by which zone information is replicated between primary and secondary servers.